LEVEL II

MITRE-Bedford

MTR-3931

AD A108828

# Industry Trusted Computer System Evaluation Process

E. T. Trotter
P. S. Tasker

1 MAY 1980









MITRE

MITRE Technical Report

MTR-3931

# Industry Trusted Computer System Evaluation Process

E. T. Trotter
P. S. Tasker

1 MAY 1980

CONTRACT SPONSOR OUSDRE (C3I)
CONTRACT NO F19628-80-C-0001
PROJECT NO 8420
DEPT. D75





THE MITRE CORPORATION
BEDFORD, MASSACHUSETTS

Department Approval: Edward H Bensley

MITRE Project Approval: Peter S. Tasker

TABLE OF CONTENTS

TABLE OF CONTENTS "Concluded"

LIST OF ILLUSTRATIONS

# SECTION 1

# INDUSTRY TRUSTED COMPUTER SYSTEM EVALUATION PROGRAM

## INTRODUCTION

### PURPOSE

The purpose of this document is to propose a process by which trusted computer system developments may be reviewed and evaluated under the DOD Computer Security Initiative Program. A trusted computer system is one which employs sufficient hardware and software integrity measures to allow its use for simultaneously processing multiple levels of classified and/or sensitive information. This document describes a process by which manufacturers may submit their proposed products for evaluation, and by which a government-wide evaluation center may conduct the review and evaluation. The criteria for evaluation of a trusted computer system are described, as well as the proposed roles of the manufacturer and the center.

### OVERALL PROGRAM

The Department of Defense Computer Security Initiative was established in 1978 with the goal of achieving the widespread availability of trusted computer systems. Three objectives must be met to accomplish this goal: 1) effectively demonstrate trusted computer systems in a variety of applications; 2) involve the commercial computer industry in the development of trusted ADP systems, and 3) establish mechanisms for evaluation of trusted ADP systems.

To accomplish the first objective, three systems are being developed. They are the Kernelized Secure Operating System (KSOS-11) for the PDP-11/70 computer, the Kernelized Virtual Machine (KVM) for the IBM-370 series computer, and KSOS-6 for a modified Honeywell level 6/43 mini-computer.

The second objective is being accomplished through the educational aspect of the initiative. Seminars and forums are an essential part of this program in order to make available research results and user requirements to stimulate computer manufacturers to develop new systems which will be suitable for trusted use by the

DoD and other government agencies.

Several elements of the third objective have already been considered. Nibaldi has proposed a set of requirements for a trusted computing base [5], and evaluation criteria [4]. Central to the implementation of an approval process is the concept of a DoD or government evaluation center. This evaluation center would perform technical "laboratory evaluations" of commercial systems to be used, or suitable for use, in federal applications requiring a trusted system. For each system evaluated, the center will produce documentation categorizing the system and describing its specific protection attributes.

## OVERVIEW

The goal of the review and evaluation process is to determine the protection provided by a computer system by comparing the features of the system to those features required for a specific level of protection as defined by Nibaldi [4].

The evaluation process will begin when a commercial computer manufacturer or a government agency requests evaluation of a computer system. Before a complete evaluation is started, the center will determine the potential the system has for use in a trusted application by examining the system documentation. If it is determined that the system is suitable, a full evaluation will be performed by the center to determine the level of protection provided by the system and ultimately to place the product on an Evaluated Products List (EPL).

It is of value to both the DoD and the manufacturer to begin the evaluation process early in the product development cycle in order to have the most beneficial effect on the protection designed into the system. To provide a context for the description of an evaluation process, section 2 defines the product development cycle for government and industry. Section 3 contains a description of the evaluation criteria and provides a basis for how the system evaluation levels are used. Finally, section 4 defines the process that will be used by the Security Evaluation Center to evaluate computer systems produced as trusted commercial products.

## SECTION 2

## DEVELOPMENT CYCLE FOR PRODUCTS

The development of computer systems is a complex process containing a series of phases. Biggs, et. al [2] provides a comprehensive description of a system development process which proceeds through four phases. The development process for DoD-contracted products is similar to that described by Biggs. One major difference is that the DoD development cycle is characterized by a series of well-defined specifications. First, a system specification which is called an A-specification, second, a development specification which is a part I or B-specification, and third, a product specification which is a part II or C-specification. A second major difference between the two development processes is in the area of design reviews and audits. For a government or DoD-contracted product a series of design reviews is required as the product progresses through the cycle. These reviews are: 1) system requirements review, 2) system design review, 3) preliminary design review, 4) critical design review, 5) functional configuration audit, and 6) physical configuration audit. For a commercial product, the design reviews and audits are internal to the developers. In general, the design team will provide design reviews to a steering committee at well-specified milestones in the development cycle.

For purposes of clarity in this paper we define the DoD-product development cycle [1] as containing four phases which are: 1) concept formulation, 2) validation, 3) full-scale engineering development, and 4) production. These phases are similar to those described by Biggs which are: 1) systems planning, 2) systems requirements, 3) systems development, and 4) systems implementation. The following paragraphs define the DoD development cycle in terms of activities that might take place in the course of commercial system development.

---

[1] Other government agencies have similar acquisition procedures, however, the DoD procedure is referenced here because it incorporates all of the critical aspects of procurement and is the one most familiar to the authors.

## CONCEPT FORMULATION PHASE

The concept formulation phase is an embryonic state where ideas are brought together to create a new system, or to modify or enhance an existing one. Ideas may originate in any part of an organization but most often are generated within marketing or engineering. Further refinement and formulation of new systems are achieved through the interaction of management, marketing, engineering, and manufacturing until the concept is complete, and a commitment is made to develop the system. Prior to making a commitment, a feasibility study may be done. Throughout the early stages of concept formulation, the manufacturer will be dealing with engineering or marketing notes, informal papers, partial documentation, and often, sensitive marketing plans and information. Ideas for new products are rigorously protected from competition throughout development, but are particularly sensitive in this early stage.

Once a commitment has been made by management to develop the system, the engineering organization will begin to prepare a system level specification for the product. This is equivalent to the DoD A-level specification defining the general nature of the system, including functional and performance requirements, and the interfaces with existing products. For a DoD or government contracted system, a System Requirements Review (SRR) will be held to determine the initial direction and progress of the contractor's system engineering effort.

## VALIDATION PHASE

This phase involves an internal review cycle with the engineering organization responsible for the product design. The development specification is usually produced during this phase. This specification describes the design of the system, including allocation of functional performance requirements to modules, and the tests required to determine compliance of the modules to the specification. The development specification is a complete statement of the performance, design, interface, and formal qualification test requirements.

If the system is to be verified to a security model, a formal Top-Level Specification must be generated as part of the development specification. This specification defines all functions visible at the user interface in a mathematically unambiguous, non-procedural, verifiable language. The verification should demonstrate that the design described by the top-level specification does not violate the rules of a security model.

This phase ends with a System Design Review (SDR) which is a final check on the system specification to ensure the completed specification adequately specifies the system requirements.

## FULL-SCALE DEVELOPMENT PHASE

In this phase, preliminary and detailed design of the system take place. In the development of a DoD contracted item, there are at least two design reviews; preliminary and critical. A Preliminary Design Review (PDR) is held after authentication of the development specification and completion of the preliminary design. This review is a formal technical review of the basic design approach. The Critical Design Review (CDR) is held after a draft product specification is produced. This specification defines how to actually build the system by specifying the exact product configuration and detailed technical description. The purpose of the CDR is to review the draft product specification and to ensure that it satisfies the performance and functional requirements established by the development specification. This review is a formal technical review of the detailed design to establish the integrity of the design prior to code and test.

## PRODUCTION PHASE

The production phase includes the actual manufacture of hardware items and the generation of software to complete the computer system. All necessary testing is performed to ensure that the system meets the technical, functional, and performance requirements of the specifications. Field support services and documentation are developed in preparation for the deployment of the system to end users. Deployment includes the actual sale and installation of the system to the customer.

Early in this phase a Functional Configuration Audit (FCA) is held to verify that development has been completed satisfactorily and that the actual system performance complies with the development specification. During this phase, the product specification is finalized. The final review of the system is the Physical Configuration Audit (PCA) which verifies that the "as built" system conforms to the technical documentation. The integrity of the product specification is established by the PCA.

## SECTION 3

## EVALUATION CRITERIA

### EVALUATION PREREQUISITES

An important requirement of the evaluation program both from the viewpoint of the manufacturer and the government is that the evaluation be consistent for all products. To achieve this, a detailed set of evaluation criteria is needed that will allow both the protection value of architectural features and the assurance value of development techniques to be well defined. In addition, it is necessary that the criteria be independent of architecture so that innovation is not impeded.

The proposed evaluation criteria and process are both generic and specific: evaluation factors have been defined, and various degrees of rigor for each factor have been incorporated into seven hierarchical protection levels representing both system-wide protection and assurance that the protection is properly implemented.

### EVALUATION FACTORS

There are three "prime evaluation factors" and numerous subsidiary factors described by Nibaldi [4]. These are listed in figure 1. The factors are independent of the architecture of the trusted system to be reviewed and evaluated, except for the "prevention" factor of "mechanism" which may be architecturally dependent. The basis for evaluation of the prevention portion of the protection mechanism is a Trusted Computing Base (TCB) (the equivalent of a security kernel and non-kernel security related software). A specification for a TCB is given by Nibaldi [5]. This specification describes the primitive operating system and ancilliary "trusted processes" that are required for a trusted system. The specification is generic in that it is applicable to the several different protection bases understood today (e.g. descriptor-based and capability-based systems). Future technological advances resulting in new system architectures may require modification of the description of a TCB, but trusted systems currently under development can be evaluated using the present TCB.

It can be expected that the detail available in the descriptions of the factors will increase and mature as the

evaluation process is applied to trusted systems under development.

Figure 1. EVALUATION FACTORS

- Policy
- Mechanism
  - Prevention
  - Detection
  - Recovery
- Assurance
  - "Development Phases"
    - Design
    - Implementation
  - "Validation Phases"
    - Testing
    - Verification
  - "Operations/Maintenance"

## PROTECTION LEVELS

The seven levels of protection proposed by Nibaldi [4] are described in figure 2. When a system is evaluated it will receive a rating determined by the highest protection level that is completely satisfied. The seven levels are cumulative in that a rating at a certain level requires that the criteria at that level and all lower levels be satisfied. Thus a system that has satisfied all of the requirements except one for a "Level 3" will be assigned a "Level 2". The results of applying the process will be to develop a list of products that have undergone evaluation, and thus are eligible for use in applications requiring a trusted system. This list of systems has been designated an evaluated products list (EPL).

LEVEL 0: NO PROTECTION

IF THERE IS NO INDICATION WITHIN THE THREE AREAS THAT A SYSTEM CAN PROTECT INFORMATION, THE SYSTEM RECEIVES A LEVEL 0 EVALUATION.

LEVEL 1: LIMITED CONTROLLED SHARING

LEVEL 1 APPLIES TO SYSTEMS WHICH HAVE DATA ACCESS CONTROLS CAPABLE OF PROVIDING ONLY LIMITED PROTECTION.

LEVEL 2: EXTENSIVE MANDATORY SECURITY

THE SYSTEM PROTECTION PROVIDES: 1) ADMINISTRATIVELY CONTROLLED AUTHORIZATION TO READ DATA, 2) FLOW CONTROL TO PREVENT DATA COMPROMISE, AND 3) WRITE ACCESS CONTROL.

LEVEL 3: STRUCTURED PROTECTION MECHANISM

THE PROTECTION MECHANISMS MUST BE CLEARLY IDENTIFIED, ISOLATED AND MADE INDEPENDENT OF OTHER SOFTWARE. TRUST IS GAINED THROUGH METHODOLOGICAL DESIGN OF THE PROTECTION-RELATED COMPONENTS OF THE OPERATING SYSTEM (I.E., THE TCB) AND MODERN PROGRAMMING TECHNIQUES. ADEQUATE TEST RESULTS ARE STILL THE PRIMARY MEANS OF ASSURANCE.

LEVEL 4: DESIGN CORRESPONDENCE

AT THIS LEVEL FORMAL METHODS ARE EMPLOYED TO CONFIRM TRUSTWORTHINESS OF THE DESIGN. MATHEMATICAL PROOFS OF CORRESPONDENCE OF THE DESIGN TO A SECURITY MODEL ARE REQUIRED.

LEVEL 5: IMPLEMENTATION CORRESPONDENCE

THE SYSTEM MUST BE SHOWN TO CORRESPOND TO THE VERIFIED TOP-LEVEL DESIGN. MORE STRINGENT REQUIREMENTS FOR DENIAL OF SERVICE, HARDWARE FAULT TOLERANCE, AND LEAKAGE CHANNEL CONTROL ARE DEMANDED.

LEVEL 6: OBJECT CODE ANALYSIS

A FORMAL ANALYSIS OF THE OBJECT CODE IS REQUIRED TO PROVE THAT THE IMPLEMENTATION SOFTWARE FULFILLS THE REQUIREMENTS OF THE SECURITY MODEL. FORMAL METHODS OF VERIFICATION MUST ALSO BE APPLIED TO THE HARDWARE.

Figure 2. TRUSTED SYSTEM PROTECTION LEVELS

## APPLICATION OF PROTECTION LEVELS

It is worth commenting on how the evaluation levels will be used by those in the government outside of the evaluation center. In order for the protection to be applied in a uniform way across many systems being procured, there must be a relatively small set of numbers describing protection that can be mapped to another relatively small set of numbers characterizing the environment into which the particular system is to be installed. The levels structure described above satisfies the requirements for simplicity and consistency. Similarly simplifying descriptive factors have been developed for the environmental risk presented by an installation or an application (in the context of the DoD classification system) by Adams [1]. Some exploration of a mapping between environmental factors and protection levels was performed during the Air Force Computer Security Summer Study [3] and the results suggest that this will be a viable way to allow various federal agencies to define their risks and to guide procurement offices in the specification of the underlying protection required for their agencies' systems.

There is a concern that reducing everything in situations as complex as these evaluations to a small set of numbers will result in a rigid and unthinking application of the numbers without consideration of the specific protection offered by a trusted system. While this is certainly possible, it is more likely that operational requirements will keep this from happening and result in the numbers being used as guideposts for both the acquisition agency and the certification authority. Thus, we would expect a procuring agency to determine that the protection offered by a "level 4" system is required for a particular system being acquired and to include such a statement in the Request for Proposal (RFP). Contractors responding to the RFP would be expected to describe their proposed system designs and how they would make proper use of the protection features of the trusted system they have chosen as the basis for their proposal. During source selection, the various bidders would be evaluated on the basis of how well they structured their application design to take advantage of the strong points in the architecture of the underlying trusted system and to minimize the weak points.

It would be possible for a bidder to propose a "level 3" system, but it would be incumbent on him to convince the source selection team that he has built his system on the strong features of the particular "level 3" system and has appropriately addressed the deficient areas. This allows the bidders to have some flexibility in their choice of systems; commensurate with the fact that they and the procuring agency will eventually have to

demonstrate to the certification authority that the proposed system satisfies the specified requirements. This also addresses the concern about a "level 3" system being "almost a level 4 system except for...".

## SECTION 4

## TRUSTED COMPUTER SYSTEM EVALUATION PROCESS

### OVERVIEW OF THE PROCESS

#### Steps of the Evaluation Process

The system evaluation process described herein consists of four sequential steps: 1) preliminary evaluation, 2) interactive evaluation, 3) final evaluation, and 4) periodic re-evaluation. The preliminary evaluation step is a determination of the suitability of an industry developed system for evaluation based upon the design of the TCB of the system. When the TCB has been adequately specified, the system will be ready for an interactive evaluation. The interactive evaluation is a review of the system design in terms of the TCB and the means by which the system satisfies the criteria for the level of protection which the manufacturer specifies. The final evaluation involves analysis and testing of the completed system to determine the level of protection provided and the strengths and weaknesses relative to that level. Periodic re-evaluation applies to those systems that are modified after a final evaluation has been completed.

#### Relationship Between the Evaluation Process and the Development Cycle

A graphic representation of the relationship between the evaluation process and the product development cycle is shown in figure 3. The evaluation process is shown as a set of four sequential steps, while the product development cycle is shown as four phases. The arrows indicate the required sequence for the evaluation of a system. The "request for evaluation" may be initiated during any of the four phases of development, but because the evaluation process is independent of the development cycle it will always consist of the four steps in sequence. A relative time line is shown to indicate that: 1) the evaluation may begin during the concept formulation phase, 2) the interactive evaluation will end when all specifications (system, development, and product) are complete, and 3) the final evaluation will take place when the system is available.

IA - 58,753

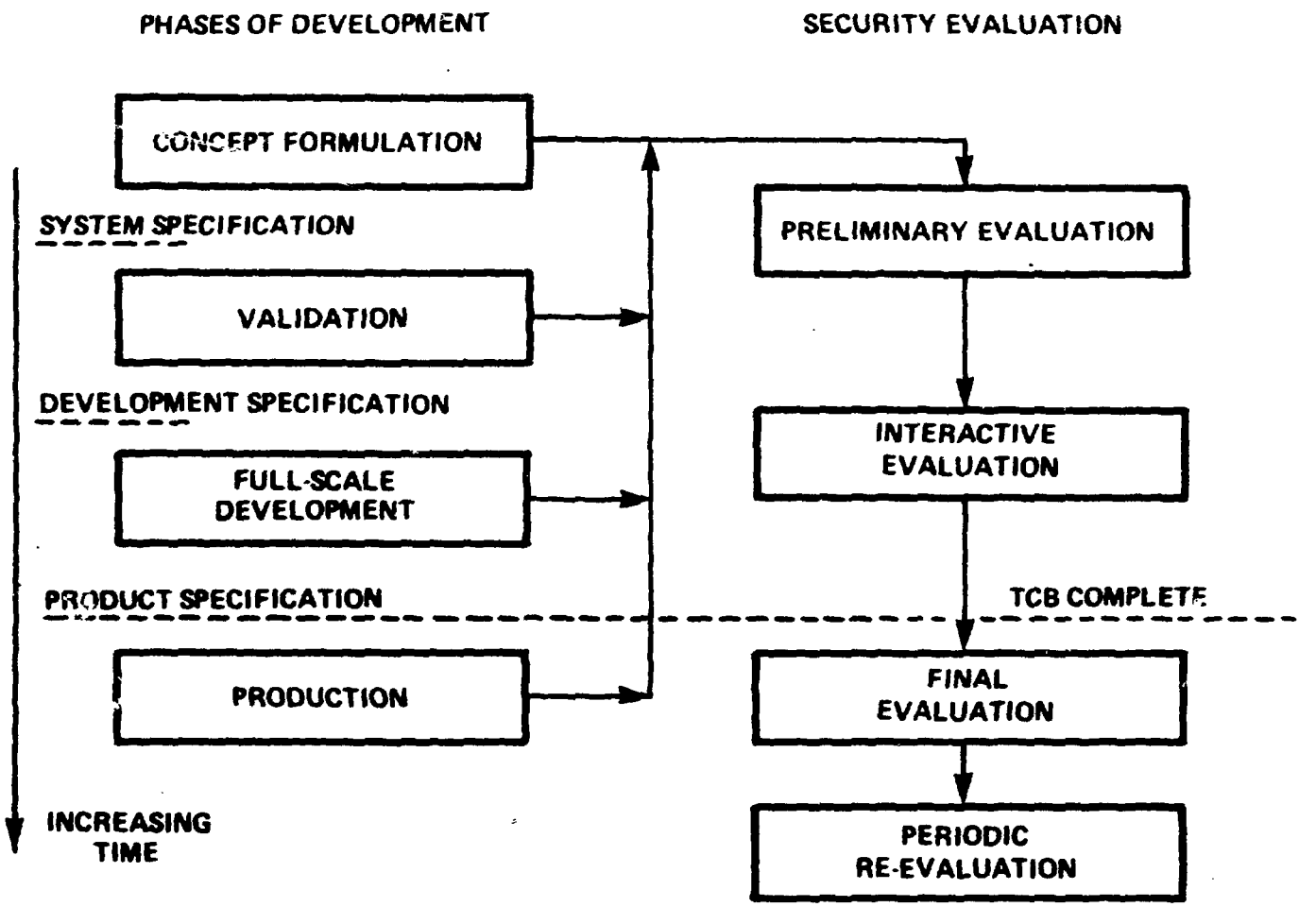


Figure 3. EVALUATION PROCEDURE

## PRELIMINARY EVALUATION

Preliminary evaluation is an analysis of the TCB of a manufacturer's system to determine the adequacy of that system for use in an environment requiring trusted access controls. The purpose of this evaluation is to determine whether or not the manufacturer's system is sufficiently designed and documented, in terms of the TCB and the evaluation criteria, to begin an interactive evaluation. When the manufacturer requests an evaluation, he will provide the evaluation center with complete system documentation and indicate the target level of protection he hopes to achieve. The documentation should describe the computer system under development in terms of the TCB specification, and detail the design and implementation of the system in terms of the technical evaluation criteria. The preliminary evaluation will determine if the TCB can possibly provide this "target" level of protection by analysis of the design methodology and the hardware and software mechanisms provided by the system.

Although it is presumed that most evaluations will be conducted on systems that have been designed with verifiable protection in mind from the onset, there may be released (production) systems that have a sufficient protection base to allow restructuring of the system to incorporate a TCB. In this case, the focus of the preliminary evaluation will be on the modifications necessary to the production system (in structure, documentation and testing) to satisfy the criteria for one of the protection levels.

In a preliminary evaluation, the developer will define the suitability of his system for use in an environment requiring a trusted computer system. His presentation will cover the areas of hardware architecture, proposed design and development methodology, verification methodology, if any, and software architecture. The manufacturer is responsible for presenting the system in a top-down fashion, and for focusing on the ways in which the system embodies the TCB and the system design satisfies the evaluation criteria for the target level of protection specified. The necessary mechanism and assurance provided by the system for the specified target level must be outlined.

When the security evaluation center receives a request to evaluate a system, a team will be formed to perform the evaluation. The output of the preliminary evaluation will be the team's assessment of the status of the system and the potential the system has of achieving the level of protection stated by the manufacturer or the highest level the system might achieve based on the information available. The assessment may indicate that the system is not yet ready to proceed to a full interactive evaluation. This

would occur if the specification has not been well defined in terms of the TCB, or if the complexity or method of implementing the TCB is not amenable to this type of evaluation. In that case, the evaluation team will identify what further information is needed, or what steps should be taken before the system is ready for interactive evaluation.

## INTERACTIVE EVALUATION

The interactive evaluation is a logical extension of the preliminary evaluation, which will begin when a preliminary evaluation indicates the product is suitable as a trusted system. The review of the system will focus on the TCB, while the review of the system design will focus on the evaluation criteria (i.e. how the design satisfies the criteria for the level of protection specified in the preliminary evaluation). The method of conducting the evaluation will be a series of presentations given by the developer, together with documentation appropriate to the level of development of the system. The government design review process which has been used for the KSOS-6 and KSOS-11 developments is the model for this interaction. The areas of hardware and software which were covered in the preliminary evaluation will now be covered in depth by the manufacturer's design team.

If the evaluation has been initiated prior to, or during, the full-scale development phase, it will occur concurrently with the development of the system. If the evaluation process is initiated later, in anticipation of subsequent releases of "trusted versions" of the system, any interactive evaluation step would take place during the manufacturer's formulation of the releases.

The role of the manufacturer in the interactive evaluation is to provide presentations and documentation on the system to the evaluation center. As in the preliminary evaluation, the focus of the presentations will be the design of the TCB and the satisfaction of the policy, mechanism, and assurance factors of the technical evaluation criteria for the manufacturer's target level of protection. The manufacturer will also determine the schedule for presentations based upon his progress in developing the system. One possible method is to tie the presentation schedule to the manufacturer's internal design review cycle. Following each internal review, the manufacturer could present a similar review for the evaluation team, but with emphasis on the TCB and the evaluation criteria. In this way, the evaluation team will be aware of the direction, methods, and conclusions pertinent to the system design, without interfering with the manufacturer's internal design review cycle, and the manufacturer will be aware of his progress relative

to the target level of protection.

The role of the evaluation team is to review the system design as presented by the designers and to point out security relevant design tradeoffs the vendor may have overlooked. The issue addressed is the compromise of the system through data security and integrity flaws, timing and storage channels, and denial of service. The evaluation team will not attempt to re-design the manufacturer's system in any way, rather, it has the responsibility to point out flaws or potential flaws to the system designers. Since the development of a computer system can extend over years, the evaluation team will provide the manufacturer with in-progress reports detailing the progress or current status of the system relative to the evaluation criteria for the target level, that is, the teams assessment of the TCB design issues, and feedback on the protection provided by the system. The evaluation team will not require the manufacturer to supply special documentation defining the TCB provided the internal documentation adequately defines the system design. KSOS-6 and KSOS-11 specifications provide examples of the type of specifications required for adequate system definition.

The interactive evaluation of an industry system will be complete when the analysis of all specifications is complete. The computer system will then be ready for final evaluation.

## FINAL EVALUATION

The final evaluation consists of analysis and testing of the production system to determine its strengths and weaknesses relative to the criteria for a specific level of protection. The developers will provide the evaluation center with a production system, or suitable access to one, and will provide details on the test methods and procedures used to determine the way in which the criteria have been satisfied for the specified level of protection. In addition, the manufacturer must show the way in which the test procedures map to the Development Specification, or to the Top-Level Specification for systems requiring verification.

The final evaluation cannot take place until the manufacturer has completed his internal acceptance testing and the system is available for field testing, so that the evaluation team will have complete access to the system for hands-on testing. There is no requirement that the evaluation occur as soon as the system is available. The manufacturer may choose to wait for some future release of the system before the final evaluation takes place.

The role of the manufacturer is to perform the actual detailed testing and where necessary, verification, to clearly demonstrate the protection capabilities of the system. Also, to aid the evaluation team's analysis of the testing, the manufacturer should provide the complete test plan and any test data requested by the evaluation center.

The evaluation team will determine what further testing is necessary, if any, to assure that the system provides the security and integrity for the specified target level, using the manufacturer's qualification testing as a starting point. The result of the final evaluation will be to determine the "actual" level of protection and to place the system in the evaluated products list. The output from the final evaluation will be in three parts: 1) a public document giving the level of the system and the possible environments where it is usable, 2) a classified flaw analysis of the system, including limitations and vulnerabilities, and where and how the system can be used, and 3) evaluation team notes.

## PERIODIC RE-EVALUATION

Computer systems, being dynamic, will be modified or enhanced at random intervals and thus will require re-evaluation. The evaluation center and manufacturer will jointly analyze all system changes to determine the security-related aspects and thus the extent of the re-evaluation needed. The higher the level of the system, the more detailed the re-evaluation will be. For example, code related changes may only effect systems of level 5 or higher where code proofs are required, while design changes will effect systems of level 4 or higher since these systems require mathematical proof of correspondence of the design to a security model.

## TIMING OF EVALUATION REQUEST

The evaluation of an industry developed computer system may start during any phase of the product development cycle. As part of the evaluation process, the center hopes that its insight and feedback to the manufacturer will tend to enhance the trustworthiness of the final system. Because of this, the earlier in the cycle the evaluation is started, the greater the protection potential for the resulting system, since the security design will be reflected in all specifications, and because there will be maximum exposure between the development team and the evaluation center. In conflict with the idea of early contact is the need for

adequate system definition and the desire of the organization to minimize exposure of its sensitive marketing plans. Ideally, the request will occur within the concept formulation phase of the product development cycle, but prior to the completion of the system specification ("A" specification). At that time the system design should be well defined in terms of the TCB.

It is important to note that high-level design information which is usually produced in the early phases of development may not exist when evaluation is started later in the development cycle. Since this information is essential to a proper evaluation, the manufacturer may find it necessary to produce specifications after-the-fact. This case will occur only for systems designed for a high level of protection.

## SECURITY EVALUATION CENTER

A DoD or government-level evaluation center is envisioned to carry out the process described above. The center will maintain a staff experienced in security issues, TCB design, system design, testing, penetration, and interaction. In addition to the evaluation of industry trusted systems, the staff will be available to government agencies requiring design or consultation on individual products or contracts, especially in the area of design of applications for trusted systems. The center will establish and maintain an internal research and development capability to enhance and create new development tools essential to the system evaluation process. Among those needed are techniques for final dynamic testing of code to show that required functions are performed properly and no unwanted functions are present. Also needed are automated tools to transform system specifications into drivers for final testing and tools to aid manual analysis of specifications. In the verification area, automated tools are needed to show correspondence proofs of source code to design, and object code to source code. A systematic, automated technique for penetration analysis is also needed. An area of research is symbolic code testing in which the execution of program paths is "simulated" through a combination of path analysis and program interpretation.

The evaluation center will be particularly sensitive to the issue of disclosure of the manufacturer's information. To prevent such disclosure, the manufacturer's documentation will be handled as sensitive or proprietary information.

The documentation produced by the center may be used by government agencies and by system contractors as input into their design and acquisition process and by accreditation authorities as

input to the accreditation process. The DoD procedures and authority for accreditation of a specific installation for classified processing remain unchanged. The interpretation of the protection features into specific threat and application environments will be done by the agency or service responsible for a particular installation. However, the resources of the center will be available to those involved in the accreditation process.

## CONFIGURATION CONTROL

Each manufacturer will provide a physically secure facility where a master copy of the software for the evaluated product will be maintained (for products of level 4 and above). The manufacturer must be able to ensure that a copy can be shown to be an exact replica of the master. For some high level products, the manufacturer will be required to provide a secure machine facility for development and testing of the trusted system.

It is incumbent upon the system developers to present as complete and comprehensive a description of the security design of the system as possible, carefully addressing the issues of policy, mechanism, and assurance as described in the security metric [4]. The proof of the design, of the existence of mechanisms, and of the verification of the system rests entirely with the developer.

## REFERENCES


[1] Adams, J., "Computer Security Environmental Considerations," Contract MDA 903-79-C-0311, IBM Corporation, Arlington, VA, August 1979.

[2] Biggs, C. L., Birks, E. G., and Atkins, W., Marketing the Systems Development Process, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1980.

[3] DeWolf, J. B., and Szulewski, P. A., (ed.), "Final Report of the 1979 Summer Study on Air Force Computer Security," The Charles Stark Draper Laboratory, Inc., Cambridge, MA, October 1979.

[4] Nibaldi, G. H., "Proposed Technical Evaluation Criteria for Trusted Computer Systems," M79-225, The MITRE Corporation, Bedford, MA, October 1979.

[5] Nibaldi, G. H., "Specification of a Trusted Computing Base," M79-228, The MITRE Corporation, Bedford, MA, November 1979.

## DISTRIBUTION LIST

INTERNAL

D-11

J. J. Croke

D-40

C. M. Sheehan

D-44

M. Ferdman

D-50

J. Mitchell

D-51

N. Briggs
C. A. Fagen

D-66

S. B. Lipner
W. Zimmer

D-70

E. L. Lafferty
W. S. Melahn

D-71

J. B. Glore
M. Hazle

D-73

J. C. C. White

D-75

S. R. Ames
D. L. Baldauf
D. Benaroya
E. H. Bensley
E. L. Burke
M. H. Cheheyl
D. L. Drake
K. B. Gasser
M. Gasser
A. Hathaway
S. W. Hosmer
G. A. Huff
J. G. Keeton-Williams
S. M. Kramer
L. J. LaPadula
C. W. McClure
J. K. Millen
G. H. Nibaldi
R. S. Popp
S. A. Rajunas
D. P. Sidhu
D. J. Solomon
J. D. Tangney
P. S. Tasker (50)
E. T. Trotter (10)
E. E. Wiatrowski
W. F. Wilson
P. T. Withington
J. P. L. Woodward

NSAHQ

R. LaBonte

W-31

D. Ault
S. E. Holmgren
S. I. Schaen
J. K. Summers
D. Wood

DISTRIBUTION LIST (Continued)

PROJECT

Communications, Command,
Control & Intelligence
Room 3B252, Pentagon
Washington, D.C. 20301

OUSDRE (C3I)

S. T. Walker (120)

APPROVED FOR PROJECT DISTRIBUTION:

Peter S. Tasker
Project Leader, 8420